Analysis of “ACK-storm” Packet

W. Eric Norum

June 11, 2003

1 Summary

A vector spectrum analyzer transmitted a malformed TCP/IP packet over its ethernet interface. The packet was received by all devices on the APS control subnet. A fault in the vxWorks network code within the IOCs and other devices on the network caused each to transmit the malformed packet again. The resulting exponential increase in network traffic completely overloaded the system, disrupted normal network operation and brought the control system to a halt.

The short-term solution is to cease communication with the offending vector spectrum analyzer. The Information Systems Support group is investigating the possibility of programming the network switches to prevent such malformed packets from being forwarded from the vector spectrum analyzer to the control system network. Wind River Systems has been informed of the fault in vxWorks.

2 Example packet

A trace of the headers of a packet making up the storm of network traffic is shown below.

```
- - - - - - - - - - - - - - - - - - - - Frame 21 - - - - - - - - - - - - - - - - - -
 Frame Status Source Address    Dest. Address      Size Rel. Time     Delta Time    A
    21        [164.54.2.68]     [164.54.2.152]       60 0:00:00.001   0.000.308     0
DLC:  ----- DLC Header -----
      DLC:
      DLC:  Frame 21 arrived at  17:55:31.5342; frame size is 60 (003C hex) bytes.
      DLC:  Destination = Multicast 01005E360298
      DLC:  Source      = Station 0030D30530C1
      DLC:  Ethertype   = 0800 (IP)
      DLC:
IP: ----- IP Header -----
      IP:
      IP: Version = 4, header length = 20 bytes
      IP: Type of service = 00
      IP:       000. ....   = routine
      IP:       ...0 .... = normal delay
      IP:       .... 0... = normal throughput
      IP:       .... .0.. = normal reliability
      IP:       .... ..0. = ECT bit - transport protocol will ignore the CE bit
      IP:       .... ...0 = CE bit - no congestion
      IP: Total length    = 40 bytes
      IP: Identification  = 48677
      IP: Flags           = 0X
```

```
24       IP:       .0.. .... = may fragment
25       IP:       ..0. .... = last fragment
26       IP: Fragment offset = 0 bytes
27       IP: Time to live    = 37 seconds/hops
28       IP: Protocol        = 6 (TCP)
29       IP: Header checksum = 8A62 (correct)
30       IP: Source address      = [164.54.2.68]
31       IP: Destination address = [164.54.2.152]
32       IP: No options
33       IP:
34 TCP: ----- TCP header -----
35       TCP:
36       TCP: Source port             = 5025
37       TCP: Destination port        = 38359
38       TCP: Sequence number         = 3201271355
39       TCP: Next expected Seq number= 3201271355
40       TCP: Acknowledgment number   = 562970529
41       TCP: Data offset             = 20 bytes
42       TCP: Flags                   = 10
43       TCP:               ..0. .... = (No urgent pointer)
44       TCP:               ...1 .... = Acknowledgment
45       TCP:               .... 0... = (No push)
46       TCP:               .... .0.. = (No reset)
47       TCP:               .... ..0. = (No SYN)
48       TCP:               .... ...0 = (No FIN)
49       TCP: Window                  = 8176
50       TCP: Checksum                = F2E8 (correct)
51       TCP: No TCP options
52       TCP:
53
```

3 Notes

1. Line 7 – The least-significant bit of first octet of the destination ethernet address is set indicating that the packet is an ethernet broadcast packet and will be received by all devices on the network.

2. Line 8 – This packet is being sent from an HP/Agilent E5810A GPIB/LAN adapter. **Many** similar packets were recorded from other devices too.

3. Line 27 – This packet has 37 more hops to continue the storm. Assuming that there are 200 devices with this bug on the network this corresponds to a theoretical generation of 200^{37} (greater than 10^{85}) more packets. Clearly this represents a 'significant' load on the network.

4. Line 30 – The IP source address is that of 'hpvecsr', an HP 89441A vector spectrum analyzer. Presumably this was the device which initiated the storm by sending the malformed packet.

5. Line 31 – The IP destination address is that of 'omicron', the IOC which was communicating with the vector spectrum analyzer.

6. Line 36 – The TCP source port is that used by the HP 89441A further strengthening the argument that it was the device which initiated the network storm.

4 Resolution

4.1 Short-term attempts

The IOC which was communicating with the vector spectrum analyzer has been stopped. This should prevent the vector spectrum analyzer from transmitting the malformed packets which precipitate the network storm. Clearly this is not an adequate long-term solution however.

A vxWorks kernel which will not perform packet forwarding has been built. This kernel will be loaded into as many IOCs as possible. This is not a true solution though since there are many IOCs with an associated MVME-162 card. These IOCs must perform packet forwarding. As well, there are devices such as the GPIB/LAN adapters over which we have no control. The result is that there will still be more than 50 devices on the network still willing to participate in a network storm.

4.2 Long-term solutions

The Information Systems Support group is investigating the possibility of adding a packet filter to the network switch which will prevent malformed packets from the HP 89441 from being forwarded to the control system network. This still leaves the possibility of some other device triggering a network storm however.

HP/Agilent has been informed of the problem in the HP 89441. A quick response seems doubtful since the device is quite old.

Wind River Systems have been informed of the problem in the vxWorks kernel. Once they provide a patch to fix the problem new kernels can be loaded into all IOCs. This will leave the GPIB/LAN adapters as the only devices willing to participate in a network storm. HP/Agilent will be informed of the problem and may be able to provide a patch to the firmware. Only when all devices on the control network have been fixed so that they no longer forward malformed packets will the network truly be safe.